NASSCOM-DSCI submission on RBI's Master Directions on PPIs

15 April 2017

Inputs on RBI's Master Directions on Issuance and Operation of Prepaid Payment Instruments in India

Overall Comments

1. NASSCOM and DSCI are grateful to the RBI for drafting guidelines for the issuance and operation of Prepaid Payment Instruments (PPI) and appreciate the process of inviting comments from stakeholders for further refinement.

2. PPIs have been instrumental in contributing to the 'less cash' vision of the Government of India. They have seen in the past six months growth far exceeding traditional payment means such as cards, especially for small transactions where they have proved to be a viable alternative to cash, especially post-demonetization.

   For instance, the top PPI/m-wallet now has 210 million users (similar to the number of customers of India's top bank) and more significantly, has 4.7 million merchants, which is around twice the number of PoS terminals installed in the country for card acceptance. In the past six months, for this PPI, users have grown 50% and the number of merchants by 800%.

   Major reasons for this growth and viability as cash alternative for micro-transactions are ease of use, ease of onboarding and customer acquisition (both user and merchant), and low PoS costs (e.g. QR code sticker instead of hardware). **In the interest of the government's less-cash vision, regulation should attempt retain these advantages of PPIs, while ensuring safety, security and reliability of transactions.**

3. NASSCOM and DSCI would wish to draw the attention of the Reserve Bank of India to the **Report of the Committee on Digital Payments – Ministry of Finance, December 2016 ('Watal Report')**, available on the Ministry of Finance website.

   The Watal Committee included RBI Executive Director Chandan Sinha, former RBI Deputy Governor H.R. Khan, and other key stakeholders from NITI Aayog, FinMin, UIDAI, IBA, NASSCOM, IAMAI, PCI and DEA, with extensive inputs from NPCI. Hence, we believe the RBI would wish to follow the recommendations of the Watal Report**.**

   In particular, we would urge the RBI to follow the **regulatory governance process** as recommended by the Watal Committee Report while issuing master directions. This would include publishing a **consultation paper** on PPIs to highlight the need for specific types of directions. Consultation paper(s) would help the stakeholders in understanding the regulator's perspective in this regard. (Ref: Watal Report page nos. 59, 157-158, 171-173). The Watal Report also recommends that all regulations be approved by a **Payments Regulatory Board** (PRB). The six-member PRB, to be headed by Governor, RBI, was subsequently announced in the Union Budget 2017.

We believe the RBI would wish to follow both letter and spirit of the progressive and landmark Watal Report, which the RBI has itself contributed so significantly to.

4. The Watal Report recommendations on digital payments should be taken into consideration. Particularly:
    a. Create parity between cash and digital payments. In the context of KYC norms, cash has relaxed compliance requirements, as against digital transactions. The Committee recommended that eKYC requirements in digital payments should be in consonance with KYC requirements in transacting in physical cash.
    b. Allow non-bank PSPs to directly access payment systems
    c. Permit telecom companies to offer Direct Carrier Billing (DCB) payment model within the telecom entity for all low value payments for all user types especially prepaid users. The threshold may be defined by RBI in consultation with TRAI and reviewed periodically.
    d. Enable payments to be inter-operable between bank and non-banks as well as within non-banks

5. **NASSCOM and DSCI and member organizations agree that security and privacy protection are very pertinent & critical to the proliferation of Digital Payment Ecosystem in the country**, and in transformation to a 'less-cash' society. Organizations are committed to ensuring security and privacy of customer data and transactions, and to mitigating security risks. We believe that **there is an urgent need to enhance Privacy Regime of the country by enacting a comprehensive Data Privacy Law in the country** to protect users, and the entire ecosystem.

6. It is critical for the PPIs to comply with a **simple, standardized and streamlined set of security-related regulatory requirements** instead of following multiple, often conflicting requirements issued by different government and regulatory bodies. MeitY has also come up with draft guidelines to be followed by PPIs.

7. Security rules for any ecosystem should be formulated and stipulated in such a way that it should not inhibit market development & its dynamics. The guidelines should be technology-agnostic, based on principles and should take into account continual technological innovation without prescribing specific security or technical solutions. Such an open, non-prescriptive approach is the most adequate in allowing PPI issuers to design and implement effective solutions to ensure continued security in an environment of evolving technology and risk. A high level security framework should be leveraged for security implementation as the implementations may vary due to factors such as size of the organization, business model and technology developments etc. In addition, adoption of globally accepted standards allow businesses to scale and stay competitive without compromising compatibility across the world (eg. One Indian PPI recently launched payment services in North America).

8. We find reference to Privacy missing in the framework. Unless RBI is planning to issue separate guidelines and framework focused on Privacy, Privacy governance and audit should be given due importance in the framework and included for protection of Personally Identifiable Information (PII) and Sensitive Personal Data or Information (SPDI) of individuals governing all aspects including Collecting, Processing, Storing, Sharing etc. of PII, thereby protecting PII at all stages of Information Lifecycle. All PPIs should also be required to publish their privacy policy on their website, app etc. Given the criticality, all PPIs should be mandatorily asked to appoint Privacy Officer (can be shared or dedicated role depending on the organizations, its scale of operations etc.), in addition to Chief Information Security Officer. A separate section on Privacy governance and audit should be included in the framework. *This applies to usual Banking Operations as well, and could be included in RBI Cyber Security Framework, unless a new Privacy Framework is already planned.*

9. **Data Breach Notification:** Not only should the regulator (RBI) and CERT be informed, but end users too should be notified in case of a Data breach. Upon knowledge, PPIs should be allowed time period of 72 hours to notify the PPI users of such a breach and necessary steps to be taken. (This applies to usual Banking Operations as well.)

10. **Cyber Security Incident Reporting:** Incident Reporting ensures that the valuable info is shared with the competent authorities in a time-bound fashion. It also affords solution and remediation to the respective enterprise which is able to counter the ill-effects of Cyber-attack or breach.

    The domain of Cyber Security incident reporting, however, has been grappling with credible challenges, and warrants some rethinking and eventually systemic change on the part of the stakeholders. First and foremost, the requirement for organizations to report to multiple agencies in the event of an attack/breach, should be revisited. At present, Banks have to report to RBI, CERT-IN (now also CERT-Fin), NCIIPC, IB-CART, in addition to their internal risk departments and the board. The reporting mechanism and structure could be made simpler, streamlined and better coordinated among various agencies. This will bolster the organizations' incident reporting agenda in turn leading to better compliance and adoption. Standardization of reporting process and format will go a long way in furthering the development of the Industry. Another pressing apprehension among the organizations is regarding the confidentiality of reported matters.

11. **Data Retention:** In addition to maintaining confidentiality and preserving Privacy, time duration for Data Retention, consistent with other regulatory provisions, should be specified for standardization.

12. Encourage PPIs to adopt 'Bug Bounty' (rewards for detecting bugs) and responsible disclosure programs to report vulnerabilities. RBI should also open a channel to receive such information, in case organization do not respond to such requests.

Specific Comments

Section 9:

- *PPIs shall be converted into full KYC semi closed PPIs within a period of 60 days from the date of issue of PPI, failing which no further credit shall be allowed in such PPIs.*
- *PPI Issuers shall ensure that all the existing minimum detail semi-closed PPIs issued by them as on the date of issue of the Master Directions, are converted into full KYC semi- closed PPIs as indicated in para 9.2 (ii) above, by June 30, 2017, failing which no further credit shall be allowed in such PPIs.*

Comment:

- Easy signup is key driver in adoption of PPIs. Requirement of KYC for each and every customer will lead to friction in the onboarding process and make it cumbersome. Low transacting users may not have enough motivation to undertake KYC. This will mean that digitally transacting customers of PPIs might be forced out of PPI network.

- Since PPIs (especially mobile wallets) require mobile number verification for use, which in turn are already KYC as per regulatory requirements and will also be linked to Aadhaar number as per new requirements, duplication of efforts for KYC can be avoided for PPIs which have verified mobile numbers.

- Requirement of full KYC (equivalent of opening a bank account) increases cost of onboarding significantly. Revenues from low value transactions are not enough to cover such costs.

- Full KYC need not be mandated for all customers. Customers with minimum KYC (authentication through OTP on mobile) should be allowed to exist. Especially as all mobile numbers are expected to be Aadhar verified. We can put additional limitations on customers not fulfilling full KYC criteria like restricting wallet to bank transfer for them.

- Further, infrastructure to undertake KYCs need to be built. It will not be possible to undertake KYC for all existing customers within 2 months. The time period to undertake KYC for existing accounts should be increased to at least 12 months. Time period to undertake KYC for new accounts should also be increased to 6 months from proposed 60 days.

Section 15.3 (a)

- *In case of wallets, PPI Issuers shall ensure that separate login is provided for the PPI account, and access to PPI is not made part of access to other services offered by the PPI Issuer or its associate / parent / group company… etc.*

Comment:

- PPI Payment system operator (PSO) should be given freedom to create workflows as per its unique business. Assignment of fraud liability against fraud / unauthorized transactions (as mentioned in the draft guidelines), products such as wallet balance insurance, entity's own technology driven fraud risk engine, among others offer customers better protection against misuse / fraud without compromising on the freedom accorded to the PSO to innovate and create customer friendly solutions.

Section 15.3 (f)

- *"Issuers shall introduce a system of additional factor of authentication for authenticating transactions in PPIs, including where PPIs are issued in the form of cards."*

Comment:

- Any additional factor of authentication which does not reduce reliability of the payment instrument may improve security. However, customer initiated additional factors reduce reliability – for example, OTP verification of transactions is likely to have high failure rates due to unreliable mobile data networks, manual input errors, etc. According to the data available, the failure rate is 15-40% for online payments using bank OTP mode of authentication. (Ref)

  Recommendation: Our recommendation is that RBI allow issuers to define methodologies to create a silent additional factor of authentication. For example, issuer can identify customers by verifying the 'fingerprint' of his device. This is

achieved by validating multiple device parameters and through advanced techniques such as canvas fingerprinting etc. We urge RBI to allow Issuers to leverage technologies like machine learning and innovate to ensure customer security while reducing friction and ensuring reliability of digital transactions.

Section 15.7

- *PPI issuers shall establish a mechanism for monitoring, handling and follow-up of cyber security incidents and cyber security breaches. The same shall be reported immediately to Reserve Bank of India. It shall also be reported to CERT-IN as per the details notified by CERT-IN.*

Comment

- Since MeitY has also made a similar requirement in recently published e-PPI guideline, it is suggested that the requirements be consolidated to help issuers use a common process for this reporting.
- Further clarification on the notification requirements on classification of incidents to be reported, format of notification, time limitation for notification, notification recipients if specified in another guideline should be referenced here to avoid confusion.

Section 17.5 (i)

- *The PPI mobile app should not be allowed to be installed on rooted devices i.e. system level access should not be allowed*

Comment

- We understand the regulator concern on securing the payment channel provided to the users specially the user device but looking at the smartphone eco-system in India specially with Android OS (Which constitute 90% plus) we recommend the regulator to focus on risk based due care approach rather than complete restriction.
- Suggestion: We encourage the regulator to let issuers make risk based decisions on allowing rooted device since there is no empirical evidence that suggests that rooted device specifically results in fraudulent activities. Moreover, there are multiple compensating controls that mitigate the risk of malware and other potential threats in a rooted device. A good example is the HKMA guidelines on Practice Note on Supervision of Stored Value Facility Licensees section 7.3.3, which warrant the safeguard of payment through user device but without recommending any direct restriction on the issuer. It recommends the issuer to implement security measures to guard against different situations including unauthorized device access, malware or virus attack, compromised or unsecure status of mobile devices and unauthorized mobile application.

Section 17.6 (viii)

- *Data loss prevention (DLP)/ Data Masking Solutions: DLP solution at end-points, network need to be implemented. Data Masking solution need to be implemented*

Comment

- Since the intent here is to protect confidentiality of data, it is suggested that instead of prescribing specific technologies like data masking, leakage prevention or encryption, the guideline should require the issuers to ensure that data is protect at rest and in transit within the issuers network and while sharing with partners for approved purposes. Controls should be implemented to prevent unauthorized access of sensitive data.